

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG
CHUYÊN NGÀNH CÔNG NGHỆ PHẦN MỀM
MÔN IOT VÀ ỨNG DỤNG



BÁO CÁO GIỮA KỲ
**ĐỀ TÀI: KHÓA CỦA THÔNG MINH NHẬN DIỆN
KHUÔN MẶT**

Giảng viên hướng dẫn : Kim Ngọc Bách
Sinh viên thực hiện :
1. Nguyễn Đức Đạt_B22DCCN195
2. Phạm Văn Đức_B22DCCN243
3. Trần Gia Hiển_B22DCCN291
4. Nguyễn Xuân Hòa_B22DCCN327
Lớp : INT14149-20251-05
Nhóm : 14

Hà Nội – 2025

MỤC LỤC

I. Giới thiệu đề tài	4
1. Mô tả dự án.....	4
2. Mục đích, ý nghĩa của dự án.....	4
3. Tổng quan phương hướng	5
4. Các thiết bị sử dụng trong hệ thống.....	5
II. Cơ sở lý thuyết và các công nghệ áp dụng	6
1. Lý thuyết về IoT	6
a. Khái niệm	6
b. Kiến trúc	6
c. Giao thức truyền dữ liệu	6
d. Bảo mật	7
e. Quản lý thiết bị	7
f. Xử lý dữ liệu	7
2. Lý thuyết về nhận diện khuôn mặt	7
a. Khái niệm	7
b. Các giai đoạn nhận diện khuôn mặt	7
c. Các phương pháp.....	8
3. Tầm quan trọng của Iot trong bảo mật bằng khóa	8
4. Cấu trúc của hệ thống khóa cửa thông minh nhận diện khuôn mặt	9
5. Giao thức truyền tin HTTP	10
6. Firebase.....	11
7. Websocket.....	12
8. Các thiết bị sử dụng trong hệ thống.....	12
a. ESP32 – CAM	12
b. Relay Module (1 kênh)	14
c. Khóa điện tử.....	15
d. FTDI232 USB to TTL conveter	16
III. Phân tích yêu cầu	17
1. Mục tiêu và phạm vi của hệ thống	17

a. Mục tiêu hệ thống	17
b. Phạm vi triển khai	18
c. Tiêu chí thành công(KPIs).....	19
d. Kết quả mong đợi	19
2. Mô tả tổng quan	19
a. Bối cảnh vấn đề	19
b. Yêu cầu từ các bên liên quan.....	20
3. Yêu cầu chức năng.....	20
4. Yêu cầu phi chức năng	21
5. Ràng buộc về kỹ thuật và môi trường	22
a. Môi trường hoạt động	22
b. Ràng buộc pháp lý	23
c. Tài nguyên thiết bị.....	24
6. Mô hình yêu cầu	24
IV. Phân tích thiết kế hệ thống	24
V. Đánh giá kết quả dự án.....	24
VI. Kết luận	24
VII. Tài liệu tham khảo.....	24

I. Giới thiệu đề tài

1. Mô tả dự án

- Hiện nay, với sự phát triển của ứng dụng điện toán đám mây và các giao tiếp không dây, việc “thông minh hóa” các hoạt động trong cuộc sống hàng ngày rất được quan tâm và phát triển. Bắt đầu từ những thói quen sử dụng điện thoại thông minh, trợ lý ảo thông minh giúp sắp xếp thời gian biểu hay thông báo lịch hẹn, hay các ứng dụng tài chính thông minh giúp cân đối tài chính cá nhân và gia đình,... Cho đến những cảnh báo tắc đường, chỉ đường khi tham gia giao thông, tất cả bây giờ đều nằm gọn trong túi quần của bạn. Và tất nhiên, không thể thiếu là hệ thống nhà thông minh, nó đang dần trở thành xu thế của thời đại. Ở đó, với 1 chiếc điện thoại thông minh cũng có thể giúp chúng ta kiểm soát ngôi nhà của mình thông qua các SMS, Email về mọi thứ ta mong muốn như nhiệt độ, bật tắt các thiết bị điện từ xa, kiểm soát tiêu thụ điện năng,... và quan trọng nhất là vấn đề an ninh của ngôi nhà của mình.
- Để giải quyết vấn đề đó, khóa cửa thông minh sinh ra để người dùng có thể bảo vệ tài sản có giá trị và đương nhiên là đáng tin cậy hơn rất nhiều các loại khóa truyền thống. Các khóa thông minh hiện nay sử dụng 3 cơ chế khóa chính là: mở khóa thẻ điện từ, mở khóa nhận diện vân tay, mở khóa bằng mật khẩu. Ngoài các loại khóa thông minh hiện nay, mở khóa bằng “nhận diện khuôn mặt” cũng là đề tài về an ninh bảo mật đang được nghiên cứu và triển khai.
- Không chỉ vậy, khóa thông minh có chức năng chính là tăng cường độ tin cậy về bảo mật, do đó nó được sử dụng vào nhiều hệ thống khác nhau như khóa cửa, khóa phòng, tủ, két sắt,....
- Với hiệu năng làm việc, cùng với độ tin cậy với tính ứng dụng cao, khóa cửa thông minh dần trở thành xu thế tất yếu của cuộc sống hàng ngày của con người.

2. Mục đích, ý nghĩa của dự án

- Nắm được cấu trúc phần cứng, sơ đồ khối, nguyên lý làm việc của mạch điều khiển.
- Tìm hiểu về lập trình với Arduino
- Biết các làm 1 đồ án hoàn chỉnh phục vụ cho việc làm đồ án tốt nghiệp.
- Hệ thống nhận diện được khuôn mặt để mở cửa tự động.
- Có thể giám sát và điều khiển từ xa qua Internet (Web).
- Có thể cập nhật firmware từ xa (OTA) cho hệ thống để bảo trì, nâng cấp tính năng mà không cần thao tác trực tiếp trên thiết bị.
- Sản phẩm nhỏ gọn mang tính thẩm mỹ cao.
- Tối ưu hóa chi phí, giá thành phù hợp với người tiêu dùng hiện nay.

- Đảm bảo bảo mật, độ chính xác cao, và hoạt động ổn định trong môi trường thực tế.

3. Tổng quan phương hướng

- Trong bối cảnh Công nghệ 4.0 và Internet of Things (IoT) phát triển mạnh mẽ, các thiết bị gia dụng, an ninh và điều khiển thông minh đang trở thành xu hướng tất yếu.
- Hệ thống khóa cửa thông minh “nhận diện khuôn mặt” là một trong ứng dụng tiêu biểu của IoT trong lĩnh vực nhà thông minh (Smart Home) và bảo mật thông minh (Smart Security).
- Cùng với sự phát triển của các công nghệ như:
 - + Trí tuệ nhân tạo AI – đặc biệt là nhận diện khuôn mặt.
 - + Điện toán đám mây (Cloud Computing).
 - + Điện toán biên (Edge Computing).
 - + Cập nhật phần mềm từ xa (OTA)
 - + Các hệ thống khóa thông minh ngày càng linh hoạt, thông minh và an toàn, giúp con người dễ dàng quản lý, kiểm soát và mở rộng chức năng.
- Phương hướng phát triển:
 - + Tích hợp trí tuệ nhân tạo giúp hệ thống phân tích dữ liệu từ cảm biến hiệu quả hơn, nhận diện được nhiều khuôn mặt phân loại tốt hơn. Mô hình học sâu tăng cường khả năng dự đoán, nhận diện chính xác hơn.
 - + Cải thiện cảm biến thông minh: Cảm biến thông minh trở nên nhỏ gọn và nhạy bén hơn, cho phép tích hợp nhiều loại cảm biến vào 1 thiết bị duy nhất.
 - + Tăng cường bảo mật: Triển khai mã hóa toàn bộ dữ liệu truyền tải, xác thực người dùng đa yếu tố, bổ sung cơ chế phát hiện xâm nhập, cảnh báo tự động qua mail / telegram.
 - + Tối ưu khả năng đăng nhập và bảo trì: Hoàn thiện hệ thống cập nhật firmware OTA qua server trung tâm, Cho phép cập nhật đa thiết bị đồng bộ qua mạng.

4. Các thiết bị sử dụng trong hệ thống

- Phần cứng:
 - + ESP32 – CAM: Bộ điều khiển tích hợp WIFI và Camera, dùng để thu hình khuôn mặt, xử lý nhận diện và điều khiển khóa cửa.
 - + Camera OV2640 (gắn sẵn trên ESP32 – CAM): Chụp hình khuôn mặt truyền cho ESP32 xử lý.
 - + Module FTDI (USB to TTL): Dùng nạp chương trình code vào ESP32 – CAM và giao tiếp UART khi code.
 - + Relay 5V: Điều khiển solenoid lock hoặc chốt cửa điện tử.
 - + Nguồn 5V 2A: Cấp cho ESP32 – CAM và các thiết bị ngoại vi.
 - + Khóa điện (12V solenoid): Thiết bị chốt mở cửa.

- + Servo motor: Cơ cấu điều khiển chốt khóa
- Phần mềm:
 - + Arduino IDE: Arduino IDE để viết mã cho ESP32. Chương trình viết xong sẽ được nạp vào ESP32 thông qua giao tiếp USB. Arduino IDE có công cụ kiểm tra lỗi và nạp chương trình để giúp đảm bảo rằng chương trình hoạt động ổn định.
 - + Arduino OTA Upload: Công cụ cập nhật phần mềm từ xa cho thiết bị qua Wifi.
 - + OpenCV + Tensorflow/Keras/Pytorch: Train mô hình nhận diện, trích xuất đặc trưng khuôn mặt.
 - + Flask / NodeJs: Xây dựng API nhận ảnh từ ESP32 – CAM, xử lý yêu cầu, quản lý dữ liệu khuôn mặt, trả kết quả.
 - + React Js: Thiết kế giao diện quản lý.
 - + MongoDB/Firebase: Lưu thông tin người dùng.
 - + MQTT Broker: Cổng giao tiếp các thiết IoT với Server.
 - + OTA update server: lưu trữ firmware mới và gửi bản cập nhật tới các thiết bị.

II. Cơ sở lý thuyết và các công nghệ áp dụng

1. Lý thuyết về IoT

a. Khái niệm

- IoT (Internet of Things) là mạng lưới các thiết bị vật lý (cảm biến, camera, vi điều khiển, thiết bị gia dụng, v.v.) được kết nối Internet để thu thập, truyền và xử lý dữ liệu.
- Trong dự án: ESP32-CAM là thiết bị IoT, có khả năng thu hình ảnh, gửi dữ liệu nhận diện đến máy chủ và nhận lệnh mở khóa từ xa.

b. Kiến trúc

Tầng	Mô tả	Ứng dụng trong dự án
Perception layer (Tầng cảm nhận)	Gồm các cảm biến, camera, actuator để thu thập dữ liệu môi trường.	ESP32-CAM (camera), relay/servo (mở khóa).
Network layer (Tầng mạng)	Truyền dữ liệu giữa thiết bị và server qua Internet (Wi-Fi, MQTT, HTTP, TCP/IP).	Wi-Fi module trên ESP32, giao tiếp MQTT/HTTP.
Application layer (Tầng ứng dụng)	Phần mềm xử lý, hiển thị, quản lý thiết bị.	Web server / app quản lý nhận diện khuôn mặt.

c. Giao thức truyền dữ liệu

Giao thức	Đặc điểm	Ứng dụng
HTTP/HTTPS	Đơn giản, dễ triển khai, nhưng tốn tài nguyên.	Gửi ảnh lên server AI để nhận diện khuôn mặt.
MQTT (Message Queuing Telemetry Transport)	Nhỏ, nhanh, tối ưu cho IoT, dựa trên publish–subscribe.	Gửi trạng thái “đã nhận diện” / “mở khóa” giữa ESP32 và server.
WebSocket	Kết nối 2 chiều thời gian thực.	Giao tiếp trực tiếp giữa server và web dashboard.

d. Bảo mật

- Xác thực (Authentication): Xác minh danh tính thiết bị/người dùng.
- Mã hóa (Encryption): Bảo vệ dữ liệu trong quá trình truyền (HTTPS, SSL/TLS).
- Phân quyền truy cập (Authorization): Chỉ cho phép người dùng hợp lệ điều khiển khóa.
- Cập nhật OTA an toàn: Firmware mới được kiểm tra chữ ký số trước khi cài đặt.

e. Quản lý thiết bị

- Device provisioning: Gán ID duy nhất cho mỗi ESP32-CAM.
- Device registration: Thiết bị đăng ký với server khi khởi động.
- Remote monitoring: Gửi dữ liệu trạng thái (online/offline, battery, signal...).
- OTA (Over-The-Air update):

f. Xử lý dữ liệu

Kiểu xử lý	Đặc điểm	Ứng dụng
Edge AI (xử lý tại thiết bị)	Xử lý ngay trên vi điều khiển, giảm độ trễ.	ESP32-CAM dùng model nhỏ (nhận diện khuôn mặt đơn giản).
Cloud AI (xử lý trên server)	Gửi dữ liệu (ảnh) lên server để AI xử lý.	Server chạy mô hình CNN nhận diện khuôn mặt chính xác hơn.

2. Lý thuyết về nhận diện khuôn mặt

a. Khái niệm

- Nhận diện khuôn mặt là quá trình phát hiện, trích xuất đặc trưng, và so sánh khuôn mặt người trong ảnh hoặc video nhằm xác định danh tính hoặc xác thực người dùng.
- Trong dự án IoT, đây là công nghệ cho phép hệ thống xác định ai đang ở trước cửa để ra quyết định mở khóa hay từ chối.

b. Các giai đoạn nhận diện khuôn mặt

Tên giai đoạn	Nhiệm vụ	Ví dụ áp dụng
Phát hiện khuôn mặt (Face Detection)	Xác định vị trí khuôn mặt trong ảnh hoặc video.	ESP32-CAM nhận dạng vùng có khuôn mặt.
Căn chỉnh khuôn mặt (Face Alignment)	Căn chỉnh khuôn mặt theo trục mắt–mũi để giảm sai lệch góc nhìn.	Xoay, cắt vùng khuôn mặt chuẩn trước khi nhận diện.
Trích xuất đặc trưng (Feature Extraction)	Biểu diễn khuôn mặt thành vector số (embedding).	Dùng CNN hoặc model MobileFaceNet.
So sánh và phân loại (Face Recognition / Matching)	So sánh vector khuôn mặt mới với cơ sở dữ liệu.	Nếu độ tương đồng > ngưỡng → mở khóa.

c. Các phương pháp

- ESP32-CAM thực hiện phát hiện khuôn mặt (face detection).
- Nhận diện (recognition) thực hiện trên server bằng mô hình machine learnig / deep learning.

3. Tầm quan trọng của IoT trong bảo mật bằng khóa

- Công nghệ IoT (Internet of Things) đóng vai trò then chốt trong việc phát triển và nâng cao bảo mật của hệ thống khóa thông minh trong thời đại công nghệ số hiện nay. Nhờ khả năng kết nối Internet và trao đổi dữ liệu theo thời gian thực, các thiết bị khóa có thể hoạt động một cách thông minh, linh hoạt và hiệu quả hơn nhiều so với khóa cơ truyền thống. Cụ thể, IoT cho phép người dùng điều khiển, giám sát và quản lý khóa từ xa thông qua smartphone, máy tính bảng hoặc máy tính, giúp kiểm soát việc ra vào nhà mọi lúc mọi nơi. Khi có hành vi đáng ngờ như truy cập trái phép, cạy khóa hay quên khóa cửa, hệ thống IoT sẽ gửi cảnh báo tức thời đến người dùng, giúp họ chủ động xử lý và bảo vệ tài sản kịp thời.
- Bên cạnh đó, IoT còn cho phép tích hợp khóa thông minh với các thiết bị an ninh khác như camera giám sát, cảm biến chuyển động, hệ thống báo cháy hoặc chuông cửa thông minh, tạo thành một mạng lưới bảo mật thống nhất và toàn diện. Nhờ khả năng thu thập và phân tích dữ liệu, hệ thống có thể học hỏi thói quen người dùng, tự động đóng mở cửa trong những thời điểm phù hợp hoặc nhận diện người dùng hợp lệ qua sinh trắc học (vân tay, khuôn mặt, giọng nói). Điều này không chỉ giúp nâng cao tính an toàn mà còn tăng sự tiện lợi và hiện đại trong quản lý an ninh nhà ở, văn phòng hay cơ sở sản xuất.

- Tóm lại, IoT không chỉ mang đến giải pháp bảo mật tối ưu và thông minh hơn, mà còn mở ra hướng phát triển mới cho ngành công nghiệp an ninh, giúp con người sống an toàn, tiện nghi và chủ động hơn trong kỷ nguyên số.

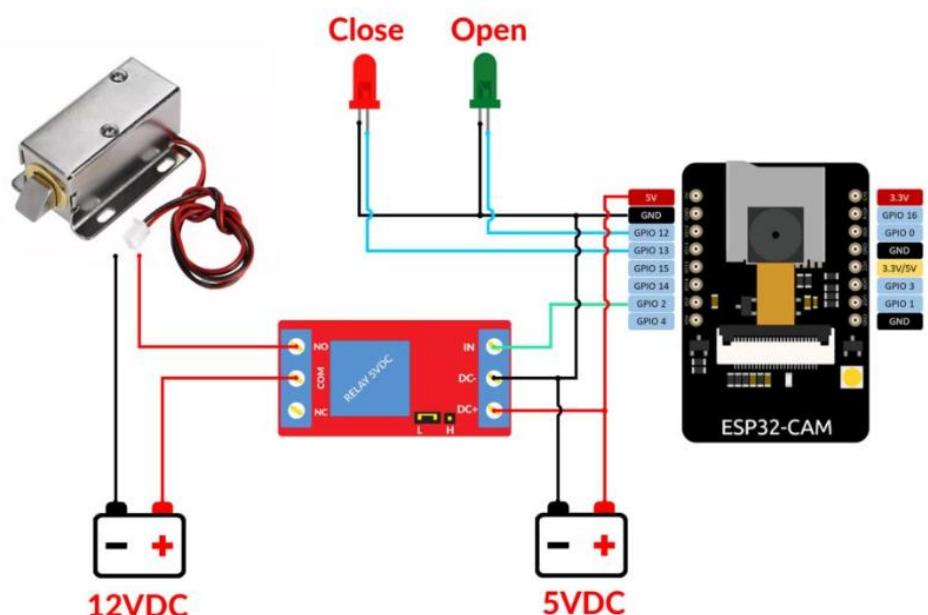
4. Cấu trúc của hệ thống khóa cửa thông minh nhận diện khuôn mặt

Hệ thống khóa cửa thông minh nhận diện khuôn mặt thường bao gồm:

- + Khối cảm biến và nhận dạng là bộ phận đầu vào quan trọng của hệ thống, chịu trách nhiệm thu thập dữ liệu khuôn mặt người dùng. Thành phần này thường sử dụng camera ESP32-CAM để chụp hình khuôn mặt khi người dùng đến gần cửa. Bên cạnh đó, cảm biến chuyển động PIR (Passive Infrared Sensor) được tích hợp để phát hiện chuyển động và kích hoạt camera khi có người xuất hiện, giúp tiết kiệm năng lượng và tăng tính tự động. Để hệ thống hoạt động hiệu quả trong điều kiện ánh sáng yếu hoặc ban đêm, cảm biến hồng ngoại (IR sensor) cũng có thể được sử dụng nhằm hỗ trợ camera nhận diện rõ nét hơn. Dữ liệu hình ảnh thu được từ camera sẽ được truyền đến bộ xử lý trung tâm để tiến hành phân tích, phát hiện và trích xuất đặc trưng khuôn mặt, phục vụ cho quá trình so sánh và nhận diện sau đó.
- + Khối xử lý trung tâm đóng vai trò là “bộ não” của hệ thống, chịu trách nhiệm phân tích, xử lý hình ảnh và ra quyết định mở hoặc khóa cửa. Bộ phận này có thể sử dụng vi điều khiển ESP32, hoặc máy tính nhúng như Raspberry Pi hay Jetson Nano nếu cần hiệu năng cao hơn. Dữ liệu hình ảnh từ camera sẽ được xử lý bằng các thuật toán phát hiện và nhận dạng khuôn mặt như Haar Cascade, MTCNN, FaceNet hoặc mô hình CNN nhẹ, được triển khai thông qua thư viện OpenCV, dlib hoặc TensorFlow Lite. Sau khi trích xuất đặc trưng khuôn mặt, hệ thống sẽ so sánh với dữ liệu khuôn mặt đã đăng ký sẵn trong cơ sở dữ liệu. Nếu khớp, bộ xử lý trung tâm sẽ gửi tín hiệu điều khiển đến khối chấp hành để mở khóa; ngược lại, nếu không khớp, hệ thống sẽ từ chối truy cập và có thể gửi cảnh báo đến người quản lý. Ngoài ra, khối này cũng có nhiệm vụ ghi lại nhật ký hoạt động và gửi dữ liệu lên máy chủ IoT để lưu trữ và giám sát từ xa.
- + Khối điều khiển và chấp hành là phần thực hiện hành động vật lý của hệ thống, tức là đóng hoặc mở khóa cửa dựa trên kết quả xử lý của khối trung tâm. Thành phần này bao gồm relay hoặc transistor điều khiển để đóng/ngắt dòng điện, khóa điện tử (solenoid lock) hoặc động cơ servo đảm nhiệm chức năng kéo – đẩy chốt cửa. Khi hệ thống xác nhận khuôn mặt hợp lệ, vi điều khiển sẽ gửi tín hiệu kích hoạt relay để mở khóa trong một khoảng thời gian nhất định, sau đó tự động khóa lại nhằm đảm

bảo an toàn. Bộ phận này cũng có thể được trang bị cảm biến trạng thái cửa (door sensor) để phát hiện tình trạng cửa đang mở hay đóng, giúp hệ thống giám sát chính xác hơn. Nguồn điện cấp cho khói chấp hành thường đến từ adapter 12V hoặc pin sạc dự phòng, đảm bảo thiết bị hoạt động ổn định và liên tục kể cả khi mất điện.

- + Khối giao tiếp và lưu trữ dữ liệu là phần kết nối hệ thống khóa thông minh với Internet, cho phép người dùng quản lý, theo dõi và điều khiển thiết bị từ xa. Thông thường, hệ thống sẽ sử dụng module WiFi tích hợp sẵn trong ESP32 hoặc các module mở rộng như ESP8266, Bluetooth BLE để kết nối với mạng Internet hoặc điện thoại thông minh. Dữ liệu nhận dạng, nhật ký truy cập, trạng thái khóa và hình ảnh chụp được sẽ được lưu trữ trên máy chủ đám mây (Cloud Server) hoặc cơ sở dữ liệu IoT như Firebase, AWS IoT, hoặc MQTT Broker. Từ đó, người dùng có thể truy cập thông qua ứng dụng di động hoặc giao diện web, để theo dõi hoạt động, thêm hoặc xóa khuôn mặt người dùng, nhận cảnh báo khi phát hiện truy cập bất thường, và thậm chí cập nhật phần mềm hệ thống từ xa. Nhờ có khối giao tiếp này, toàn bộ hệ thống hoạt động theo mô hình IoT hoàn chỉnh – thông minh, an toàn và dễ dàng mở rộng.



5. Giao thức truyền tin HTTP

- Khái niệm: Giao thức truyền thông Hypertext Transfer Protocol (HTTP) là một giao thức cơ bản được sử dụng để truy cập và truyền tải dữ liệu trên Internet. Trong lĩnh vực IoT, HTTP đóng vai trò quan

trọng trong việc kết nối và truyền thông dữ liệu giữa các thiết bị IoT và các hệ thống backend.

- HTTP được dùng làm giao thức giao tiếp giữa thiết bị IoT và máy chủ đám mây. Khi camera ESP32-CAM nhận diện được khuôn mặt, dữ liệu hình ảnh hoặc kết quả nhận dạng sẽ được gửi đến máy chủ qua HTTP Request (thường là phương thức POST hoặc PUT). Ngược lại, người dùng có thể điều khiển mở khóa, thêm người dùng mới, hoặc xem nhật ký truy cập thông qua HTTP Response từ máy chủ gửi về. HTTP giúp thiết bị và ứng dụng trao đổi thông tin nhanh chóng, dễ triển khai và tương thích với hầu hết các nền tảng IoT hiện nay.
- Khi người dùng đến gần cửa, camera ESP32-CAM sẽ tự động chụp hình khuôn mặt và gửi dữ liệu hình ảnh đó đến API trên máy chủ thông qua yêu cầu HTTP POST để kiểm tra tính hợp lệ. Máy chủ sau khi nhận dữ liệu sẽ tiến hành so sánh với cơ sở dữ liệu khuôn mặt đã lưu trữ và phản hồi kết quả bằng HTTP Response. Nếu khuôn mặt được xác định là hợp lệ, thiết bị sẽ nhận lệnh mở khóa và kích hoạt relay để điều khiển cơ cấu chốt cửa hoạt động. Ngược lại, nếu khuôn mặt không trùng khớp, hệ thống sẽ giữ nguyên trạng thái khóa và có thể gửi cảnh báo về ứng dụng quản lý thông qua giao thức HTTP hoặc MQTT, giúp người dùng phát hiện các truy cập bất thường. Bên cạnh đó, người quản trị hệ thống cũng có thể tương tác với máy chủ qua các API RESTful sử dụng HTTP, chẳng hạn như gửi yêu cầu GET để truy vấn danh sách người dùng đã đăng ký, POST để thêm khuôn mặt mới vào cơ sở dữ liệu, hoặc DELETE để xóa quyền truy cập của một người dùng khỏi hệ thống.
- Trong hệ thống khóa cửa thông minh nhận diện khuôn mặt, Client chính là thiết bị IoT như ESP32-CAM hoặc vi điều khiển trung tâm, có nhiệm vụ gửi yêu cầu HTTP đến Server thông qua các API endpoint được định nghĩa sẵn. Khi nhận được yêu cầu, Server (có thể là máy chủ đám mây hoặc máy chủ nội bộ) sẽ xử lý dữ liệu, tiến hành truy vấn cơ sở dữ liệu để kiểm tra thông tin khuôn mặt, đồng thời thực hiện các thao tác xác thực hoặc điều khiển theo yêu cầu của thiết bị. Sau khi hoàn tất xử lý, Server sẽ phản hồi kết quả về cho thiết bị thông qua HTTP Response, trong đó dữ liệu phản hồi được định dạng ở dạng JSON (JavaScript Object Notation) – một cấu trúc dữ liệu nhẹ, dễ phân tích và truyền tải giữa thiết bị IoT và ứng dụng. Nhờ đó, quá trình giao tiếp giữa thiết bị và máy chủ diễn ra nhanh chóng, rõ ràng và thuận tiện cho việc mở rộng hoặc tích hợp thêm các chức năng điều khiển, giám sát từ xa.

6. Firebase

- Khái niệm: Firebase trong IoT là một nền tảng được sử dụng để hỗ trợ lưu trữ và quản lý dữ liệu của các thiết bị IoT trên đám mây.

Firebase cung cấp một loạt các dịch vụ, chẳng hạn như cơ sở dữ liệu thời gian thực, lưu trữ tệp, phân tích, và khả năng xác thực người dùng, giúp các hệ thống IoT có thể lưu trữ, xử lý và đồng bộ dữ liệu dễ dàng giữa các thiết bị và ứng dụng.

- Các khía cạnh chính về việc sử dụng Firebase trong dự án IoT:
 - + Firebase Realtime Database: là một giao thức được xây dựng dựa trên WebSocket và HTTP để cung cấp kết nối dữ liệu liên tục theo thời gian thực, là một cơ sở dữ liệu NoSQL, nơi mà dữ liệu được lưu trữ dưới dạng JSON và đồng bộ hóa theo thời gian thực. Điều này rất phù hợp với các ứng dụng IoT, vì các thiết bị IoT thường cần gửi và nhận dữ liệu trong thời gian thực.
 - + Firebase Cloud Messaging (FCM): cho phép các thiết bị IoT gửi và nhận thông báo thông qua dịch vụ đám mây của Firebase. Ví dụ, một thiết bị IoT có thể phát hiện sự cố (như phát hiện khói hoặc khí gas vượt ngưỡng) và gửi thông báo tới người dùng ngay lập tức.
 - + Firebase Hosting: có thể được sử dụng để lưu trữ ứng dụng web, trang điều khiển các thiết bị IoT, giúp quản lý và điều khiển thiết bị từ xa qua giao diện người dùng (UI).

7. Websocket

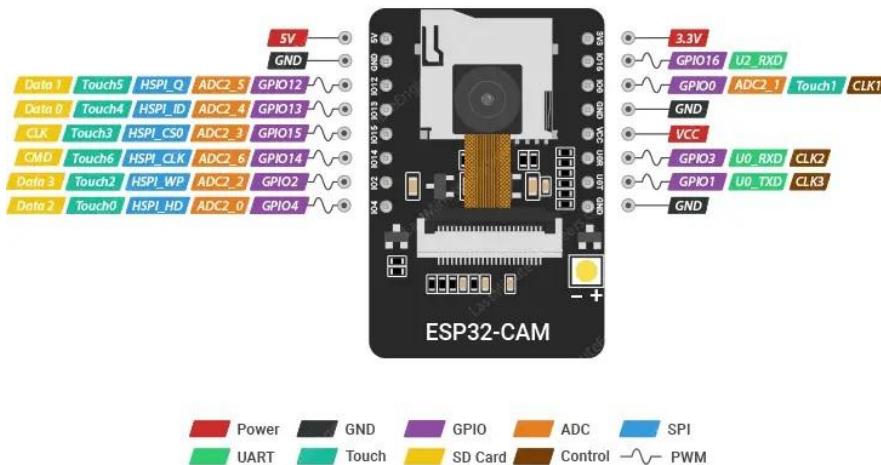
- Khái niệm: WebSocket là một giao thức truyền thông cung cấp các kênh liên lạc song công hoàn toàn qua một kết nối TCP duy nhất giữa máy khách và máy chủ. Không giống như HTTP truyền thống tuân theo mô hình phản hồi yêu cầu, giao thức này cho phép giao tiếp hai chiều. Điều này có nghĩa là máy khách và máy chủ có thể gửi dữ liệu cho nhau bất cứ lúc nào, giúp dữ liệu được truyền đi nhanh chóng mà không cần phải tải lại trang web.
- Cách hoạt động:
 - + Client (thiết bị IoT) gửi yêu cầu mở kết nối WebSocket tới server qua HTTP.
 - + Server chấp nhận kết nối và thiết lập một kênh giao tiếp hai chiều.
 - + Sau khi kết nối được thiết lập, cả hai bên có thể truyền dữ liệu lẫn nhau mà không cần gửi thêm yêu cầu HTTP mới.
 - + Khi không còn dữ liệu, kết nối sẽ vẫn mở cho đến khi một trong hai bên ngắt kết nối.

8. Các thiết bị sử dụng trong hệ thống

a. ESP32 – CAM

- ESP32-CAM có một camera kích thước nhỏ, rất cạnh tranh trong ngành, giống như mô-đun chính, mô-đun này có thể được xử lý công việc độc lập, module có kích thước nhỏ gọn chỉ 40 x 27 x 12 mm, dòng nghỉ chỉ 6mA.

- ESP-32CAM có thể được sử dụng rộng rãi trong các ứng dụng IoT khác nhau, thích hợp cho thiết bị thông minh gia đình, điều khiển không dây công nghiệp, giám sát không dây kiểm soát, nhận dạng không dây QR, tín hiệu hệ thống định vị không dây...Nó là một giải pháp lý tưởng cho các ứng dụng IoT
- Mạch thu phát Wifi BLE ESP32 này là mạch chính hãng AI – Thinker có chất lượng độ ổn định và độ bền rất cao, sử dụng camera OV2640 chất lượng cao hình ảnh sắc nét, không nhiễu sọc, không xảy ra tình trạng treo khi hoạt động do sử dụng ic cấp nguồn chất lượng cao.
- Mạch thu phát Wifi BLE ESP32-CAM Ai-Thinker này có thể sử dụng Arduino IDE để biên dịch và viết code, được hỗ trợ mạnh mẽ từ cộng đồng.



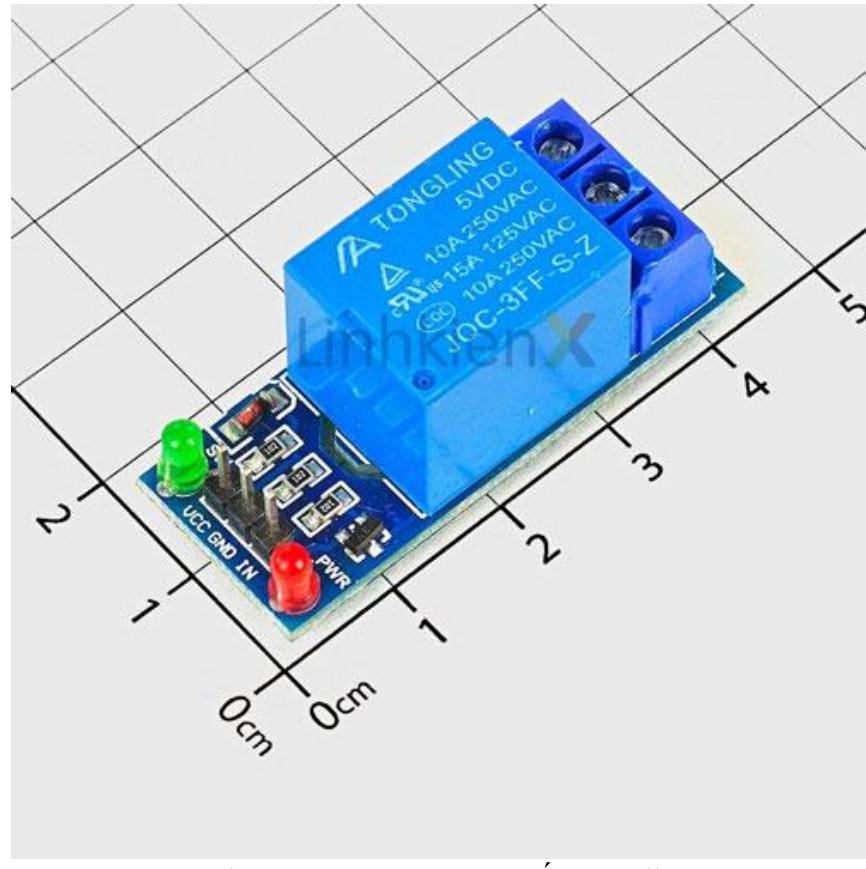
- Cấu tạo:
 - + Power (Chân nguồn): Có hai chân nguồn là 5V và 3V3. Chúng ta có thể cấp nguồn cho ESP32-CAM qua một trong hai chân này. Vì nhiều người dùng đã gặp phải sự cố khi cấp nguồn cho thiết bị ở mức 3,3V, nên ESP32-CAM luôn được cấp nguồn qua chân 5V. Chân VCC thường xuất ra 3,3V từ bộ điều chỉnh điện áp trên bo mạch. Tuy nhiên, nó có thể được cấu hình để xuất ra 5V bằng cách sử dụng liên kết Zero-ohm gần chân VCC.
 - + GND: Nối đất
 - + GPIO: Trên ESP32-S có tổng 32 chân GPIO, nhưng có một số chân được dùng nội bộ cho PSRAM và máy ảnh nên chúng ta chỉ còn lại 10 chân có thể sử dụng. Trong đó, mỗi chân lại có 1 nhiệm vụ ngoại vi khác nhau, chẳng hạn như SPI, UART, ADC hoặc Touch.
 - + UART: Trên thực tế, ESP32-S có hai giao diện UART là UART0 và UART2. Tuy nhiên, chân RX (GPIO 16) của

UART2 bị hỏng, khiến chúng ta chỉ có thể dùng UART0 trên ESP32-CAM (GPIO 1 và GPIO 3). Ngoài ra, do ESP32-CAM thiếu cổng USB nên các chân này phải dùng để bật đèn flash cũng như kết nối với các thiết bị UART như GPS, cảm biến vân tay, cảm biến khoảng cách,... tùy theo nhu cầu người dùng.

- + MicroSD: Dùng để kết nối thẻ nhớ microSD. Nếu không sử dụng thẻ nhớ microSD, bạn có thể sử dụng các chân này làm đầu vào và đầu ra thông thường.
- + ADC: Các chân ADC2 được trình điều khiển WiFi sử dụng nội bộ nên chúng không thể được sử dụng khi đang bật Wi-Fi.
- + Touch: ESP32-CAM có 7 GPIO cảm ứng điện dung. Khi tải điện dung (chẳng hạn như ngón tay người) ở gần GPIO, ESP32 sẽ phát hiện sự thay đổi điện dung.
- + SPI: ESP32-CAM chỉ có một SPI (VSPI) ở chế độ phụ và chế độ chính.
- + PWM: ESP32-CAM có 10 kênh (tất cả các chân GPIO) PWM được điều khiển bởi bộ điều khiển PLC. Đầu ra PWM có thể được sử dụng để điều khiển động cơ kỹ thuật số và đèn LED.

b. Relay Module (1 kênh)

- Module Relay là một thiết bị điện tử giúp chuyển mạch bằng cách sử dụng tín hiệu điều khiển điện áp thấp để điều khiển các thiết bị điện công suất cao. Relay đóng vai trò như một công tắc điều khiển từ xa, cho phép bật/tắt các thiết bị điện mà không cần tiếp xúc trực tiếp. Nhờ đó, relay được sử dụng rộng rãi trong các hệ thống tự động hóa, nhà thông minh và IoT.
- Module Relay 1 kênh: Điều khiển một thiết bị duy nhất, thường được sử dụng trong các ứng dụng đơn giản như bật/tắt đèn, quạt hoặc bơm nước.



- Relay hoạt động dựa trên nguyên tắc của điện từ trường. Khi dòng điện chạy qua cuộn dây, nó tạo ra một từ trường hút hoặc nhả tiếp điểm bên trong relay. Nhờ đó, relay có thể đóng hoặc mở mạch điện đầu ra, giúp điều khiển các thiết bị điện lớn bằng tín hiệu điều khiển điện áp thấp.
- Cấu tạo:
 - + Cuộn dây (Coil): Là bộ phận tạo từ trường khi có dòng điện chạy qua, quyết định khả năng đóng/mở của relay.
 - + Tiếp điểm (Contacts): Thành phần quan trọng giúp relay đóng/mở mạch điện, điều khiển trực tiếp thiết bị.
 - + Diode bảo vệ: Giúp ngăn chặn dòng ngược từ cuộn dây, tránh làm hỏng vi điều khiển.
 - + Mạch cách ly (Optocoupler, Transistor): Đảm bảo sự an toàn và ổn định của tín hiệu điều khiển, giảm thiểu nhiễu điện.
 - + LED báo trạng thái: Hiển thị trạng thái hoạt động của relay, giúp người dùng dễ dàng kiểm tra.

c. Khóa điện tử

- Khóa chốt điện tử LY-03, có chức năng hoạt động như một ổ khóa cửa sử dụng Solenoid để kích đóng mở bằng điện, được sử dụng nhiều trong nhà thông minh hoặc các loại tủ, cửa phòng, cửa kho,... khóa sử dụng điện áp 12VDC, là loại thường đóng (cửa đóng) với chất lượng tốt, độ bền cao. Khóa chốt điện tử này có thể

sử dụng chung với các mạch chức năng tạo thành một hệ thống thông minh.

12V 0.6A

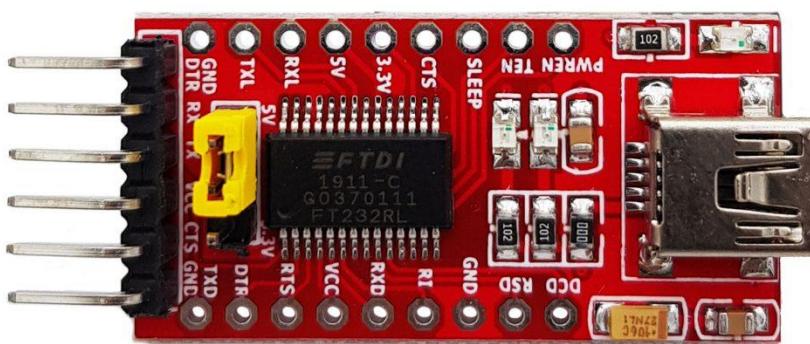


- Thông số kỹ thuật
 - + Vật liệu: Thép không gỉ
 - + Nguồn điện: 12V DC
 - + Dòng điện làm việc: 0.6A
 - + Công suất: 9.6W
 - + Yêu cầu nguồn cấp: 12VDC/1A
 - + Kích thước: L54 x D38 x H28
 - + Thời gian cấp nguồn: Nhỏ hơn 10s

d. FTDI232 USB to TTL converter

- Mạch chuyển USB UART TTL FT232RL sử dụng IC FT232RL từ chính hãng FTDI, mạch được thiết kế nhỏ gọn nhưng vẫn ra chân đầy đủ, rất dễ sử dụng với mọi hệ điều hành Windows, Mac, Linux.
 - + Chip có sẵn ổn áp và dao động tích hợp bên trong, hoạt động rất ổn định so với các dòng chip USB to serial khác
 - + Mạch có thể hoạt động ở 2 chế độ 5v hoặc 3v3, bằng cách thiết lập trên jumper trên mạch

- + Chân cắm ra gồm 2 loại theo chuẩn FTDI (phù hợp với Arduino) và chuẩn UART thường, được ký hiệu rõ ràng trên mạch. Đầu vào sử dụng loại USB B mini.
- + Ngoài ra, trên mạch có sẵn 2 led cho tín hiệu TX và RX, giúp theo dõi trực tiếp trạng thái tín hiệu.



- Thông số kỹ thuật:
 - + IC chính: FT232RL chính hãng FTDI
 - + Nguồn cấp: 5VDC từ cổng USB (cổng mini USB hoặc USB Type-C)
 - + Có ngõ ra nguồn có thể điều chỉnh 3V3 hoặc 5VDC
 - + Chuyển giao tiếp từ USB sang UART TTL
 - + Drive hỗ trợ Windows Mac, Linux
 - + Có cầu chì tự phục hồi: 500mA
 - + Tốc độ Baudrate: tùy chỉnh
 - + Kích thước PCB: 36 x 18.5mm
 - + Trọng lượng: 3g

III. Phân tích yêu cầu

1. Mục tiêu và phạm vi của hệ thống

a. Mục tiêu hệ thống

- Vấn đề thực tế: Khóa cửa cổ điển, mặc dù đã được sử dụng phổ biến trong thời gian dài, hiện nay đang bộc lộ nhiều hạn chế trong bối cảnh nhu cầu bảo mật và tự động hóa ngày càng cao. Việc phụ thuộc hoàn toàn vào chìa khóa vật lý khiến người dùng dễ gặp rắc rối khi làm mất hoặc quên chìa, thậm chí chìa có thể bị sao chép một cách dễ dàng, gây ra nguy cơ mất an toàn. Hơn nữa, khóa cơ học không có khả năng ghi lại lịch sử truy cập hay xác định ai đã mở cửa và vào thời điểm nào, điều này gây khó khăn cho việc quản lý trong các môi trường như văn phòng, chung cư hay nhà thông minh. Quá trình cấp hoặc thu hồi quyền truy cập cũng thủ công, mất thời gian và thiếu linh hoạt. Ngoài ra, khóa cổ điển không thể tích hợp với các hệ thống tự động hóa hoặc thiết bị IoT khác, khiến người dùng không thể giám sát, điều khiển từ xa hay kết hợp với các tính năng an ninh nâng cao. Dù có độ bền cơ học nhất định, khóa truyền thống vẫn có thể bị phá bằng các công cụ chuyên dụng và hoàn toàn thiếu các lớp bảo mật thông minh như sinh trắc học hay xác thực đa yếu tố. Chính vì những hạn chế này, nhu cầu chuyển đổi sang các hệ thống khóa thông minh nhận diện khuôn mặt đang trở nên tất yếu, nhằm mang lại sự tiện lợi, an toàn và quản lý hiệu quả hơn trong kỷ nguyên IoT hiện nay.
- Mục tiêu dự án IoT này mang lại: hệ thống khóa cửa thông minh nhận diện khuôn mặt ứng dụng IoT là tạo ra một giải pháp bảo mật hiện đại, tiện lợi và tự động hóa cao nhằm thay thế cho các loại khóa truyền thống. Cụ thể, dự án hướng đến việc tăng cường an toàn thông qua công nghệ nhận diện khuôn mặt – giúp đảm bảo chỉ những người được cấp quyền mới có thể mở khóa, loại bỏ nguy cơ bị sao chép chìa khóa hoặc mất thẻ từ. Bên cạnh đó, hệ thống còn cho phép kết nối Internet, giúp người dùng giám sát và điều khiển cửa từ xa thông qua ứng dụng di động hoặc trình duyệt web, đồng thời nhận cảnh báo tức thời khi có truy cập trái phép. Ngoài ra, dự án cũng nhằm mục tiêu nâng cao khả năng quản lý và mở rộng, thông qua việc lưu trữ và xử lý dữ liệu trên nền tảng đám mây, cho phép người quản trị dễ dàng thêm, xóa hoặc cập nhật quyền truy cập của người dùng. Về mặt học thuật và kỹ thuật, dự án giúp người phát triển hiểu rõ hơn về công nghệ IoT, hệ thống nhúng, giao tiếp mạng, xử lý ảnh và trí tuệ nhân tạo, từ đó góp phần ứng dụng vào thực tế, phục vụ cho xu hướng nhà thông minh và tự động hóa trong thời đại 4.0.

b. Phạm vi triển khai

- Số lượng thiết bị (Mô hình nhà 1 cửa _ gia đình):
 - + ESP32-CAM: 1.
 - + Relay Module (1 kênh): 1

- + Khóa điện tử: 1.
- + Nguồn 5V + nguồn 12V: 1 bộ
- + FTDI USB-TTL: 1
- Môi trường hoạt động:
 - + Điều kiện vật lý: Ngoài trời, cần vỏ kín chống bụi, chống nước, chống ngưng tụ và cách điện. Nếu lắp nơi có điều kiện khắc nhiệt hơn, cần phần cứng chịu nhiệt / vị trí che chắn.
 - + Nguồn điện:
 - + ESP32-CAM: nguồn 5V DC, $\geq 2A$.
 - + Khóa: Thường là 12V DC, cần cấp nguồn riêng hoặc bộ nguồn dùng chung có phân nhánh.
 - + Bảo vệ nguồn: dùng fuse, diode flyback cho coil, transient suppressor (TVS) nếu đường dài.
 - + Mạng và kết nối:
 - + Wifi: RSSI tối ưu $> -70 \text{ dBm}$; nếu yêu cầu AP gần/mesh wifi.
 - + Băng thông: stream camera MJPEG/ snapshot — định kỳ gửi ảnh lớn.
 - + Độ tin cậy: router/AP ổn định, QoS cho MQTT nếu nhiều thiết bị.

c. Tiêu chí thành công(KPIs)

- Độ chính xác: Sai số nhận diện khuôn mặt $< 2\%$.
- Độ trễ: Ghi nhận khuôn mặt và gửi lên server trong vòng $< 5s$.
- Độ tin cậy: Tỉ lệ truyền dữ liệu thành công $> 95\%$, hoạt động ổn định trong thời gian dài, chịu được các yếu tố của môi trường, thông báo khi xảy ra lỗi.
- Tiết kiệm tài nguyên: Tối ưu hóa việc sử dụng năng lượng, bộ nhớ, băng thông khi truyền dữ liệu.
- Chi phí: Giảm thiểu chi phí lắp đặt, bảo trì và vận hành, hướng đến 1 giải pháp khả thi, dễ triển khai cho đến cả các hộ gia đình và doanh nghiệp nhỏ.
- Khả năng mở rộng: Thiết kế hệ thống có cấu trúc linh hoạt, dễ dàng thêm mới các tính năng trong tương lai.

d. Kết quả mong đợi

- An toàn trong việc bảo vệ tài sản của gia đình và doanh nghiệp.
- Có thể giám sát từ xa qua thiết bị di động.
- Dữ liệu được truyền ngay lập tức, cảnh báo khi có hành vi không an toàn.

2. Mô tả tổng quan

a. Bối cảnh vấn đề

- Trong khuôn khổ gia đình và các doanh nghiệp có nhiều các vật dụng đáng giá mà bảo mật chũ tối ưu.
- Hiện nay, việc bảo mật an ninh thủ công -> dễ bị khai thác bởi những kẻ gian do không thể kiểm soát được, thiệt hại về kinh tế.
- Đề xuất một thiết bị IoT có khả năng bảo vệ an toàn cho gia đình và doanh nghiệp, vừa có khả năng giám sát từ xa.

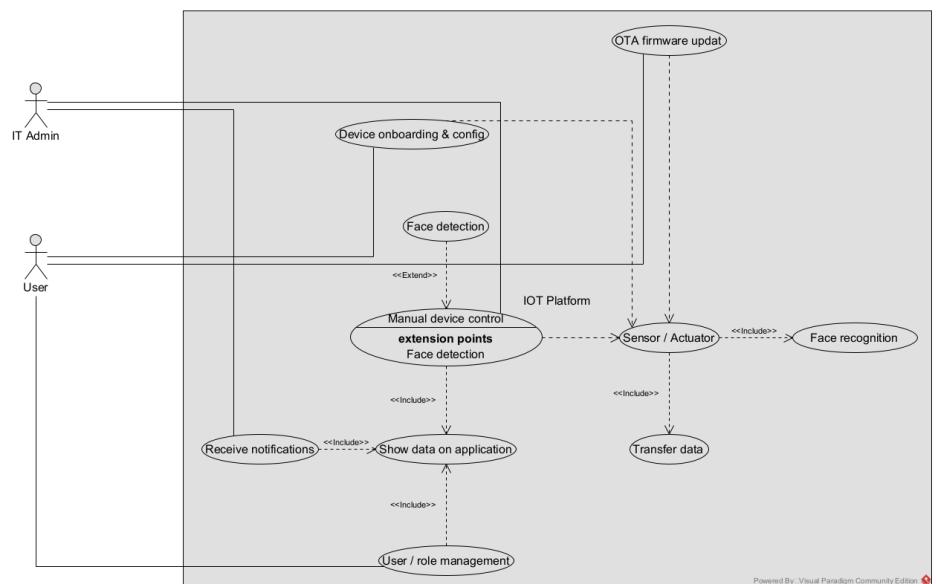
b. Yêu cầu từ các bên liên quan

- Người dùng cuối:
 - + Hệ thống dễ sử dụng, thao tác mở/khóa cửa nhanh chóng và thân thiện.
 - + Đảm bảo an toàn và bảo mật cao, tránh truy cập trái phép.
 - + Có thể điều khiển và giám sát từ xa qua điện thoại hoặc máy tính.
 - + Cung cấp thông báo thời gian thực (real-time) khi cửa mở, đóng hoặc phát hiện truy cập bất thường.
 - + Hệ thống hoạt động ổn định, ít lỗi, độ trễ thấp.
 - + Thiết bị có thiết kế gọn gàng, thẩm mỹ, phù hợp với không gian nhà ở.
- Doanh nghiệp, quản lý:
 - + Dễ dàng triển khai, lắp đặt và bảo trì cho khách hàng.
 - + Có thể quản lý và theo dõi thiết bị của nhiều khách hàng thông qua hệ thống quản trị tập trung (dashboard).
 - + Hỗ trợ tích hợp mở rộng với các dịch vụ IoT khác (nhà thông minh, camera giám sát, cảm biến chuyển động...).
 - + Chi phí sản xuất và vận hành hợp lý, có khả năng thương mại hóa.
 - + Có hệ thống cập nhật phần mềm và bảo mật từ xa (OTA) để giảm chi phí bảo trì trực tiếp.
- Kỹ thuật, IT:
 - + Thiết kế hệ thống có kiến trúc linh hoạt, dễ mở rộng và nâng cấp.
 - + Hỗ trợ giao tiếp giữa các module (MCU, cảm biến, bộ truyền thông) một cách hiệu quả, tiết kiệm năng lượng.
 - + Đảm bảo độ tin cậy, độ chính xác và độ trễ thấp khi xử lý tín hiệu điều khiển.
 - + Áp dụng các giao thức truyền thông IoT phổ biến (như MQTT, HTTP hoặc WebSocket).
 - + Tích hợp hệ thống bảo mật dữ liệu và xác thực người dùng.
 - + Có công cụ giám sát, ghi log và xử lý sự cố để dễ dàng bảo trì sau này.

3. Yêu cầu chức năng

- Các chức năng cần có:

- + Thu thập dữ liệu từ cảm biến.
- + Gửi dữ liệu về gateway/cloud.
- + Lưu trữ và phân tích dữ liệu.
- + Hiển thị dữ liệu qua ứng dụng.
- + Điều khiển / ra lệnh ngược lại thiết bị.
- + Cập nhật Firmware
- + Quản lý người dùng và quyền truy cập
- + Nhận thông báo
- + Quản lý đăng ký khuôn mặt
- + Nhận diện khuôn mặt
- Đặc tả luồng công việc:
- + Use case:



4. Yêu cầu phi chức năng

- Hiệu năng:
 - + Độ trễ phản hồi: Thời gian từ khi người dùng gửi lệnh mở/khóa cửa đến khi cửa phản hồi không vượt quá 2 giây trong điều kiện mạng ổn định (<100ms ping).
 - + Tốc độ xử lý tín hiệu tại thiết bị: Vi điều khiển phải xử lý tín hiệu điều khiển trong vòng <100ms kể từ khi nhận lệnh.
 - + Dung lượng lưu trữ log: Thiết bị lưu trữ tối thiểu 100 bản ghi truy cập gần nhất (thời gian, người dùng, trạng thái cửa).
 - + Tần suất gửi dữ liệu: Gói tin trạng thái được gửi lên server 10s 1 lần hoặc ngay khi có thay đổi trạng thái.
- Bảo mật:
 - + Truyền thông an toàn: Dữ liệu giữa thiết bị và máy chủ được mã hóa bằng TLS 1.2 hoặc cao hơn.

- + Xác thực người dùng: Yêu cầu mật khẩu ≥ 8 ký tự, chữ hoa, chữ thường, số, ký tự đặc biệt. Phiên đăng nhập tự động hết hạn sau 15' hoạt động.
- + Quản lý truy cập: Chỉ người dùng có quyền truy cập hợp lệ mới có thể điều khiển thiết bị. Ghi lại lịch sử truy cập.
- Độ tin cậy:
 - + Thời gian hoạt động: Hệ thống đảm bảo 98% thời gian hoạt động mỗi tháng.
 - + Khả năng phục hồi: Sau khi mất kết nối mạng, hay mất điện hệ thống tự khởi động và kết nối lại trong vòng $\leq 20s$.
 - + Xử lý lỗi: Hệ thống ghi log lỗi, tự động gửi cảnh báo lên server khi gặp sự cố. Dữ liệu không bị mất trong trường hợp gian đoạn mạng ngắn hạn ($< 30s$).
- Khả năng mở rộng:
 - + Hệ thống máy chủ hỗ trợ tối thiểu 1000 thiết bị hoạt động đồng thời.
 - + Có thể hoạt động trên 10000 thiết bị mà không cần thay đổi kiến trúc hệ thống, chỉ cần mở rộng tài nguyên phân cứng.
 - + Có thể hỗ trợ thêm các module IoT khác thông qua API mở.
- Chi phí & năng lượng:
 - + Nguồn điện:
 - Nguồn điện cho toàn bộ thiết bị khóa cửa IoT cần đảm bảo ổn định, liên tục và an toàn.
 - Hệ thống thường sử dụng nguồn một chiều (DC) 5V hoặc 12V.
 - Nếu cấp điện liên tục từ lưới 220V, cần dùng biến áp và mạch ổn áp (adapter chuyển 220V AC \rightarrow 5V/12V DC) để tránh quá tải hoặc dao động điện áp gây hỏng linh kiện.
 - + Băng thông:
 - Triển khai thực tế, cần đăng ký dịch vụ lưu trữ của 1 bên thứ 3, tùy vào gói đăng ký sẽ nhận được lưu lượng tương ứng để lưu trữ hình ảnh thu nhận trong 1 khoảng thời gian xác định (tối thiểu 50MB / ngày).
 - + Chi phí hạ tầng:

Khoảng 20.000vnd / thiết bị / tháng, ở mức 5000 thiết bị \rightarrow Dùng MQTT + serverless analytics cho workload biến động.

5. Ràng buộc về kỹ thuật và môi trường

a. Môi trường hoạt động

- Nhiệt độ & độ ẩm: cảm biến đặt ngoài trời, chịu được biến độ -10°C đến 45°C, độ ẩm $> 90\%$. \rightarrow Cần chọn thiết bị chống nước IP67, vỏ bọc chống bụi.

- Nhiều sóng:
 - + Thiết bị IoT thường dùng Wi-Fi / Bluetooth / RF 2.4 GHz, dễ bị nhiễu bởi:
 - + Lò vi sóng, router Wi-Fi khác, thiết bị Bluetooth, hoặc nguồn cao tần.
 - + Cản bỏ trí khoảng cách tối thiểu 0.5–1 m với các thiết bị gây nhiễu mạnh.
 - + Thiết kế mạch và vỏ kim loại cần có lớp chống nhiễu (EMC shielding) để đảm bảo tín hiệu ổn định.
 - + Có thể áp dụng lọc nguồn (LC filter) và tách mass digital/analog để giảm nhiễu.
- Nguồn cấp:
 - + Nguồn điện cần ổn định và bảo vệ quá áp:
 - + Nguồn vào: 220 V AC (nguồn lưới).
 - + Nguồn ra cấp cho thiết bị: 5 V DC (vi điều khiển, cảm biến), 12 V DC (motor/servo).
 - + Sử dụng biến áp cách ly hoặc adapter switching (220 V → 12 V/2A) để tránh quá tải.
 - + Cần tụ lọc (100 µF – 470 µF) và diode bảo vệ ngược cực trong mạch nguồn.
 - + Trong trường hợp mất điện, nên có pin dự phòng hoặc UPS mini (5 V – 12 V) đảm bảo hệ thống hoạt động 2–6 giờ.

b. Ràng buộc pháp lý

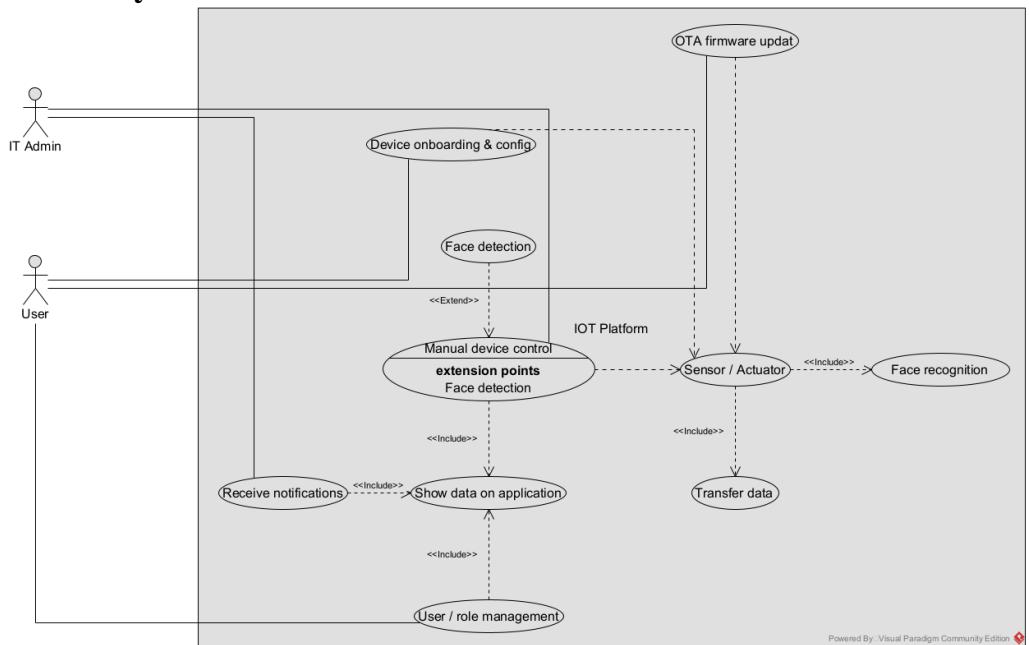
- Tần số vô tuyến
 - + Thiết bị sử dụng Wi-Fi (2.4GHz hoặc 5GHz), Bluetooth, hoặc các giao thức truyền thông tầm ngắn khác phải hoạt động trong dải tần được cấp phép bởi Bộ Thông tin & Truyền thông Việt Nam (MIC).
 - + Không được phát công suất vượt quá giới hạn cho phép (≤ 100 mW đối với Wi-Fi 2.4GHz).
 - + Khi triển khai thực tế, thiết bị cần được kiểm định tương thích điện tử (EMC) và có tem chứng nhận hợp quy (CR).
- Bảo mật dữ liệu
 - + Dữ liệu khuôn mặt, tên người dùng, và lịch sử truy cập là thông tin nhạy cảm theo Nghị định 13/2023/NĐ-CP về bảo vệ dữ liệu cá nhân.
 - + Việc thu thập, lưu trữ và xử lý dữ liệu phải có sự đồng ý rõ ràng của người dùng.
 - + Dữ liệu phải được mã hóa trong quá trình lưu trữ và truyền tải (AES, SSL/TLS).
 - + Người dùng có quyền yêu cầu chỉnh sửa, xóa dữ liệu hoặc rút lại sự đồng ý bất cứ lúc nào.

- An ninh mạng
 - + Tuân thủ Luật An ninh mạng 2018: bảo đảm an toàn thông tin khi kết nối Internet, không để lộ lõi hỏng gây truy cập trái phép.
 - + Hệ thống phải có cơ chế xác thực và phân quyền truy cập (admin, người dùng, khách).
 - + Phải có biện pháp chống tấn công mạng, như tường lửa phần mềm, chống giả mạo yêu cầu (CSRF, XSS), và giám sát đăng nhập bất thường.

c. Tài nguyên thiết bị

- Hệ thống sử dụng vi điều khiển (như ESP32) với CPU ≥ 160 MHz, RAM ≥ 300 KB, Flash ≥ 8 MB để đảm bảo xử lý nhận diện khuôn mặt ổn định.
- Nguồn cấp DC 5V–12V, dòng tiêu thụ khoảng 400–1000 mA, cần adapter ổn áp, chống nhiễu và pin dự phòng 2–6 giờ khi mất điện.
- Toàn hệ thống phải tối ưu tài nguyên để vừa đảm bảo hiệu năng, vừa tiết kiệm năng lượng và bảo vệ linh kiện.

6. Mô hình yêu cầu



IV. Phân tích thiết kế hệ thống

V. Đánh giá kết quả dự án

VI. Kết luận

VII. Tài liệu tham khảo

